RSAC 2025 Conference

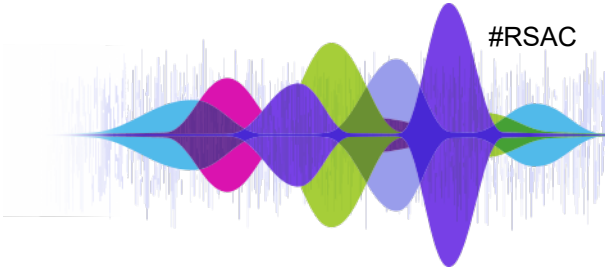
Many Voices.
One Community.

SESSION ID: HUM-M03

Information As A Domain of War

Colonel (Retired) Lawrence D. Dietz, Esq., U.S.

General Counsel
Tal Global
https://www.linkedin.com/in/lawrencedietz/

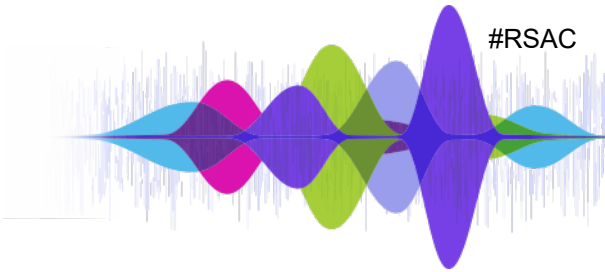


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.



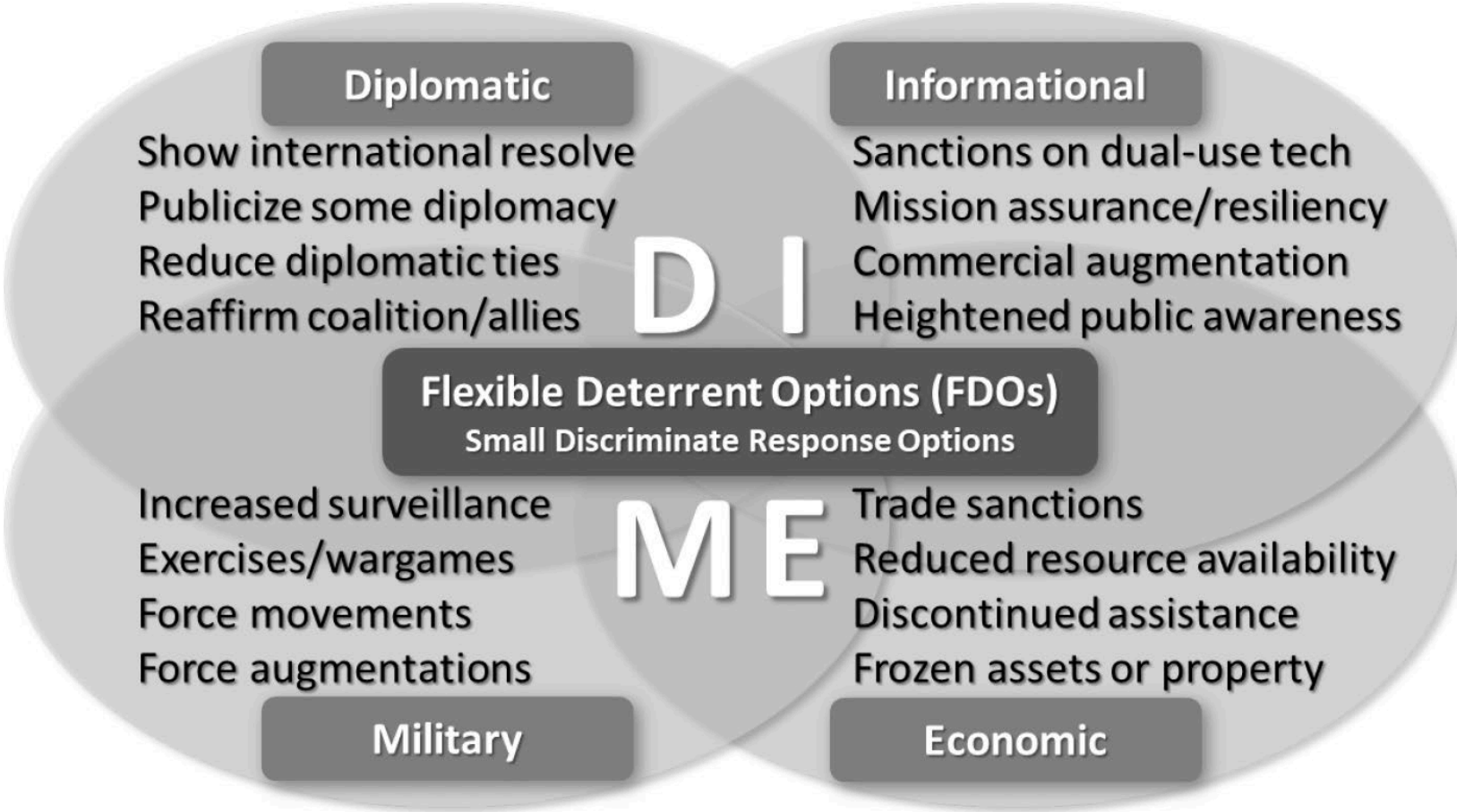
Agenda

- Overview – What Are The Domains of War
- Instrumentalities of Statecraft
- Information Operations – Orchestrating Non-Kinetic Systems on the Battlefield
- IO in Ukraine
- IO in Gaza
- Nation State Disinformation
- Enterprise Influence Operations

Multi-Domain Operations in NATO

Source" https://www.act.nato.int/article/mdo-in-nato-explained/

Instrumentalities Of Statecraft

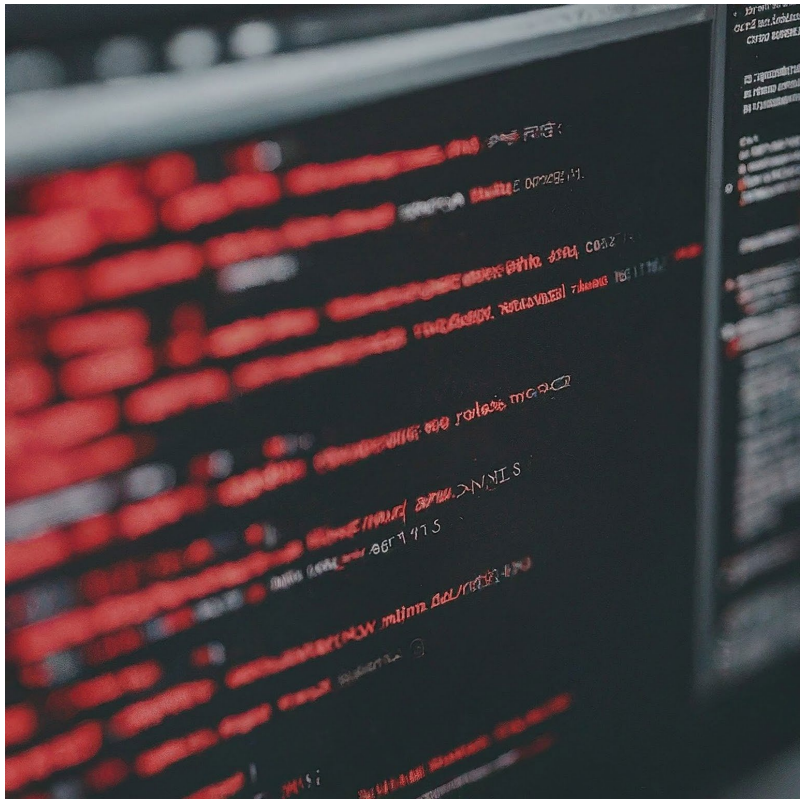


Source: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-141/MP-SAS-141-17.pdf

TALGLOBAL
Trusted Expert Solutions
Security Consulting ◆ Risk Management

RSAC 2025 Conference

Kinetic Vs. Non-Kinetic Weapon



Military Information Operations

- Key Components:
  - Psychological Operations
  - Cyberspace Operations
  - Electronic Warfare (Jamming)
  - Public Affairs
  - Civil Military Operations
  - Propaganda

Source: JP 3-13 2012

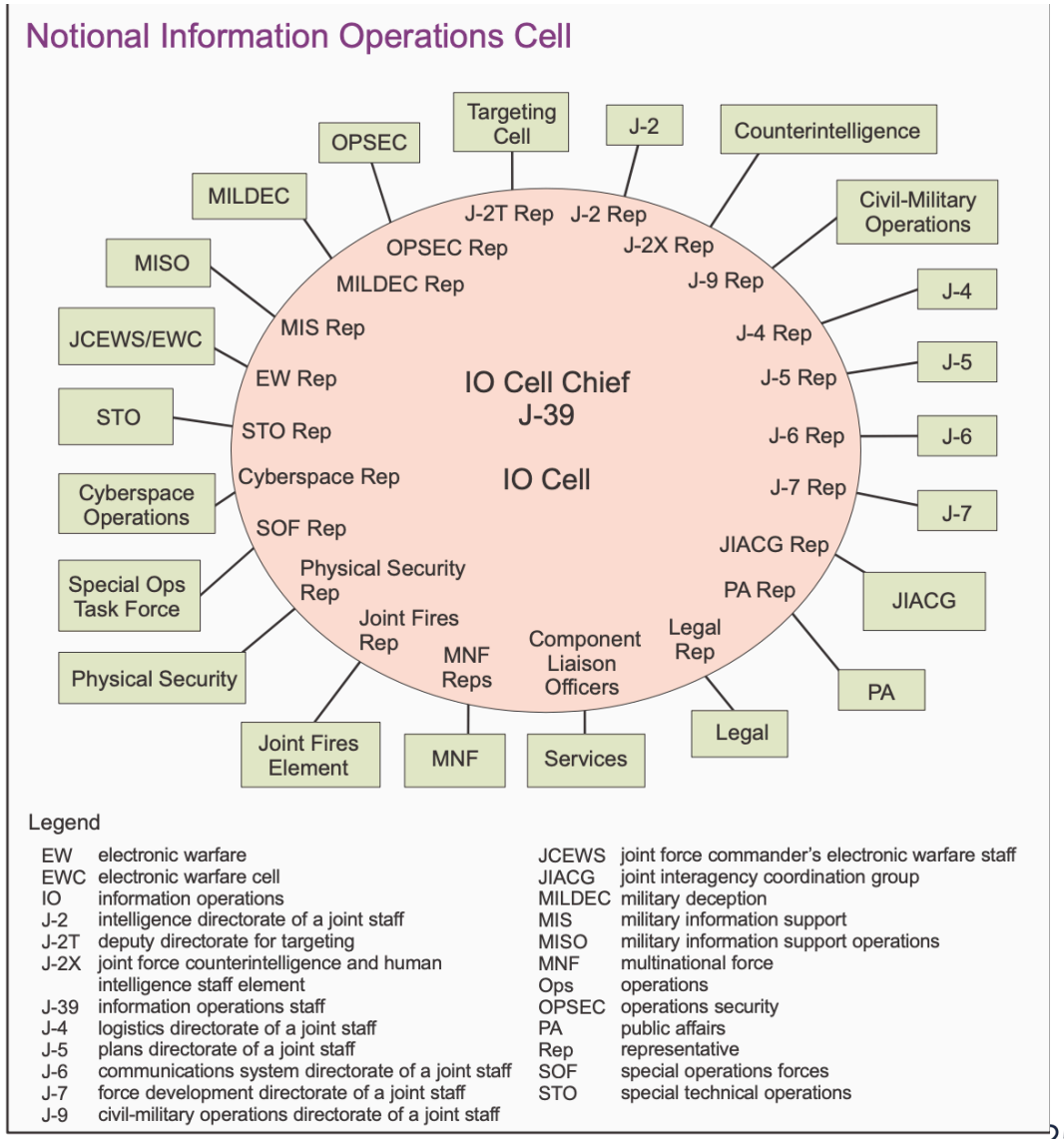


Figure II-3. Notional Information Operations Cell

TALGLOBAL
Trusted Expert Solutions
Security Consulting ◆ Risk Management

IO In Ukraine - PSYOP

Ukraine doubles down on psychological campaign against North Korean troops

A TV screen shows file images of North Korean soldiers during a news program at Seoul Railway Station in Seoul, South Korea, Oct. 18, 2024.

Source: https://www.voanews.com/a/ukraine-doubles-down-on-psychological-campaign-against-north-korean-troops/7847270.html

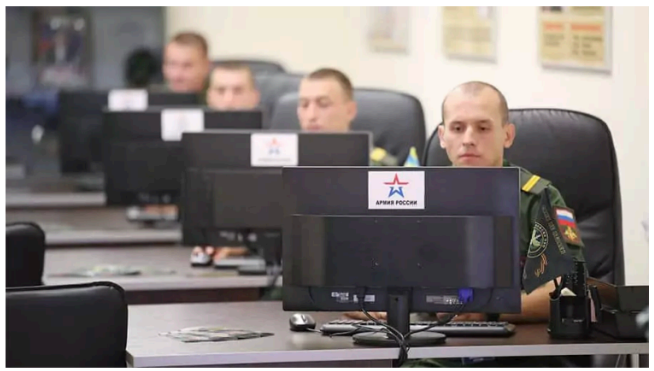
IO In Ukraine - PSYOP

Airstrikes, Artificial Intelligence, and Sabotage Drive Russian Psyops

Publication: Eurasia Daily Monitor Volume: 21 Issue: 117

By: Yuri Lapaiev

August 1, 2024 05:53 PM Age: 7 months



(Source: Izvestiya)

Executive Summary:

- The Russian Federation continues its efforts aimed at destabilizing Ukrainian society and undermining Kyiv's defense capabilities through the use of social media and bots to spread disinformation.
- Russian propagandists effectively combine kinetic and non-kinetic means to increase the effects on the target audience, embellishing Russian military victories and the declining state of Ukrainian infrastructure.
- The focus on exploiting mobilization issues and energy blackouts as primary disinformation targets highlights the Kremlin's intention to sow discord and weaken Ukraine from within.

Source: https://jamestown.org/program/airstrikes-artificial-intelligence-and-sabotage-drive-russian-psyops/

IO In Ukraine - PSYOP

Source:
https://www.forbes.com/sites/davidaxe/2024/03/15/a-russian-psyops-vehicle-rolled-toward-avdiivka-trying-to-lure-ukrainians-into-captivity-it-didnt-work/

A Russian Psyops Vehicle Rolled Toward Avdiivka, Trying To Lure Ukrainians Into Captivity. It Didn't Work.

Soldiers in Ukraine have a good reason for resisting calls to surrender.

By David Axe, Forbes Staff. David Axe writes about ships, planes, tanks, drones a... Follow Author

Published Mar 15, 2024, 07:58pm EDT, Updated Mar 15, 2024, 10:07pm EDT

Save Article Comment 39

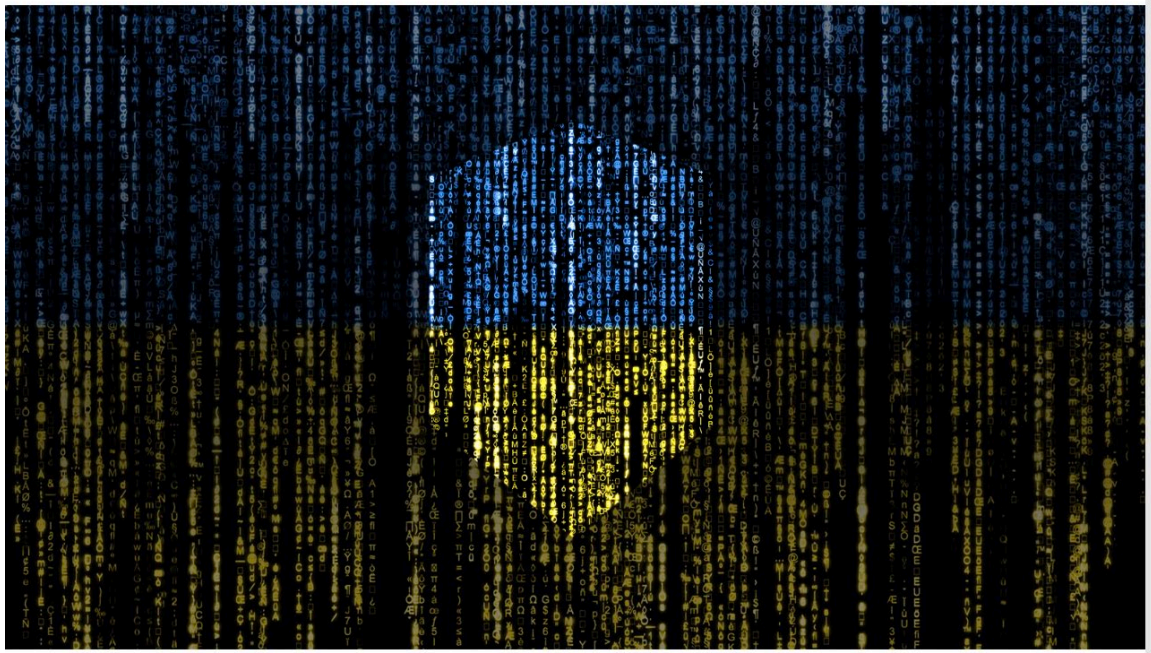
A Russian ZS-88 around Avdiivka. VIA AFV RECOGNITION

As the grueling, four-month battle for the industrial city of Avdiivka in eastern Ukraine culminated in mid-February, the Russian armed forces—which up to that point mostly had relied on glide-bombs, artillery and infantry-first "meat assaults" to soften the Ukrainian garrison—tried something different.

IO In Ukraine – Cyber War

Defending Ukraine: Early Lessons from the Cyber War

Jun 22, 2022 | Brad Smith - Vice Chair & President



Source: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

IO In Ukraine – Cyber War

Source: https://www.forbes.com/sites/thomasbrewster/2025/02/11/usaid-was-a-big-help-in-ukraines-cyber-war-with-russia-not-any-more/

EDITORS' PICK

The Wiretap: USAID Was A Big Help In Ukraine's Cyber War With Russia. Not Any More.

By Thomas Brewster, Forbes Staff. Senior writer at Forbes covering cybercrime, ... Follow Author

Published Feb 11, 2025, 01:56pm EST, Updated Feb 12, 2025, 10:39am EST

Save Article Comment 0

The Wiretap is your weekly digest of cybersecurity, internet privacy and surveillance news. To get it in your inbox, subscribe here.

(Photo by Kayla Bartkowski/Getty Images) GETTY IMAGES

IO In Ukraine – Electronic Warfare

Source: https://www.c4isrnet.com/electronic-warfare/2024/05/06/electronic-warfare-in-ukraine-has-lessons-for-us-weapons-navigation/

Electronic warfare in Ukraine has lessons for US weapons, navigation

By **Colin Demarest**

May 6, 2024

A rocket sits in a field near grazing cows on April 10, 2022, in Ukraine. (Anastasia Vlasova/Getty Images)

IO in Gaza – PSYOP

Source:
https://www.iranintl.com/en/202404158853

Leaked Document Reveals IRGC's Role In Global Anti-Israel Campaign

Iran International Newsroom

Apr 15, 2024, 21:28 GMT+1

Share

A scene of a pro-Palestinian rally in Paris, France, October 22, 2023

IO in Gaza - Cyberwar

Source: https://theconversation.com/a-look-inside-the-cyberwar-between-israel-and-hamas-reveals-the-civilian-toll-228847

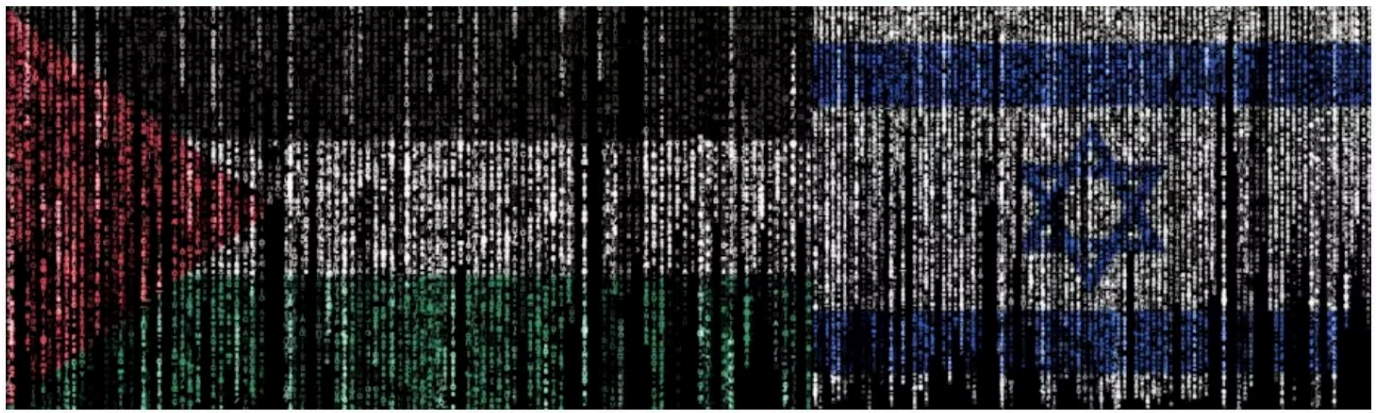
THE CONVERSATION

Academic rigor, journalistic flair

Arts + Culture | Economy | Education | Environment + Energy | Ethics + Religion | Health | Politics + Society | Science + T

A look inside the cyberwar between Israel and Hamas reveals the civilian toll

Published: May 3, 2024 8:16am EDT



The conflict between Israel and Hamas is happening online as well as on the ground. Gwengoat/iStock / Getty Images Plus

IO by Russia Exploiting Gaza

ANALYSIS
How Russia uses the Israel-Gaza Crisis in its disinformation campaign against the West
08 Dec 2023
Short Read by Maria Shamraj

Source: https://icct.nl/publication/how-russia-uses-israel-gaza-crisis-its-disinformation-campaign-against-west

Russia: US Presidential Election

Source: https://www.bbc.com/news/articles/c8rx28v1vpro

BBC

Watch Live

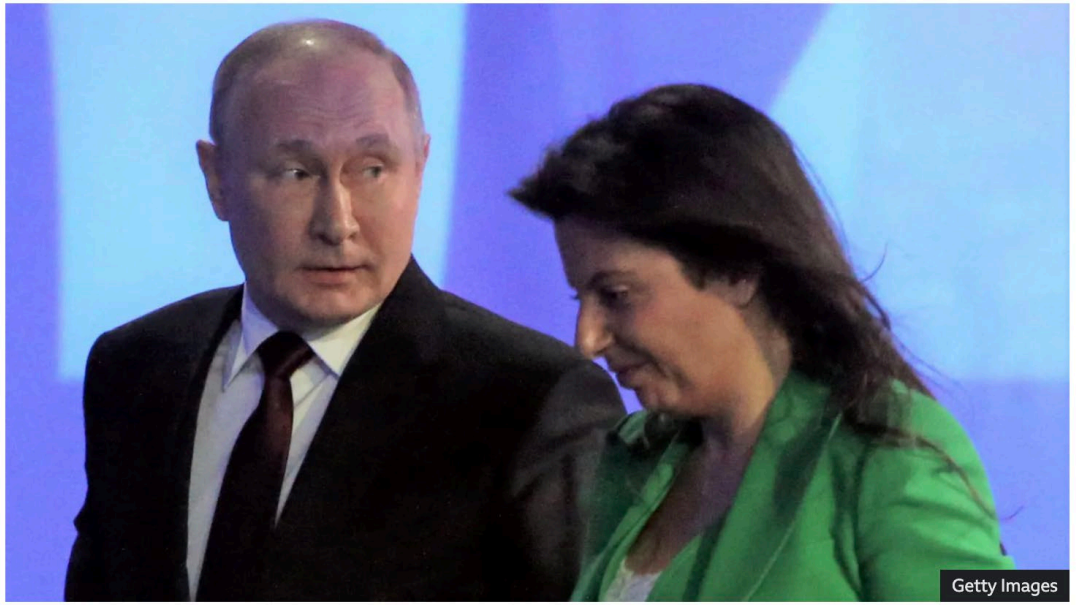
Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

US accuses Russia of 2024 election interference

4 September 2024

Share Save

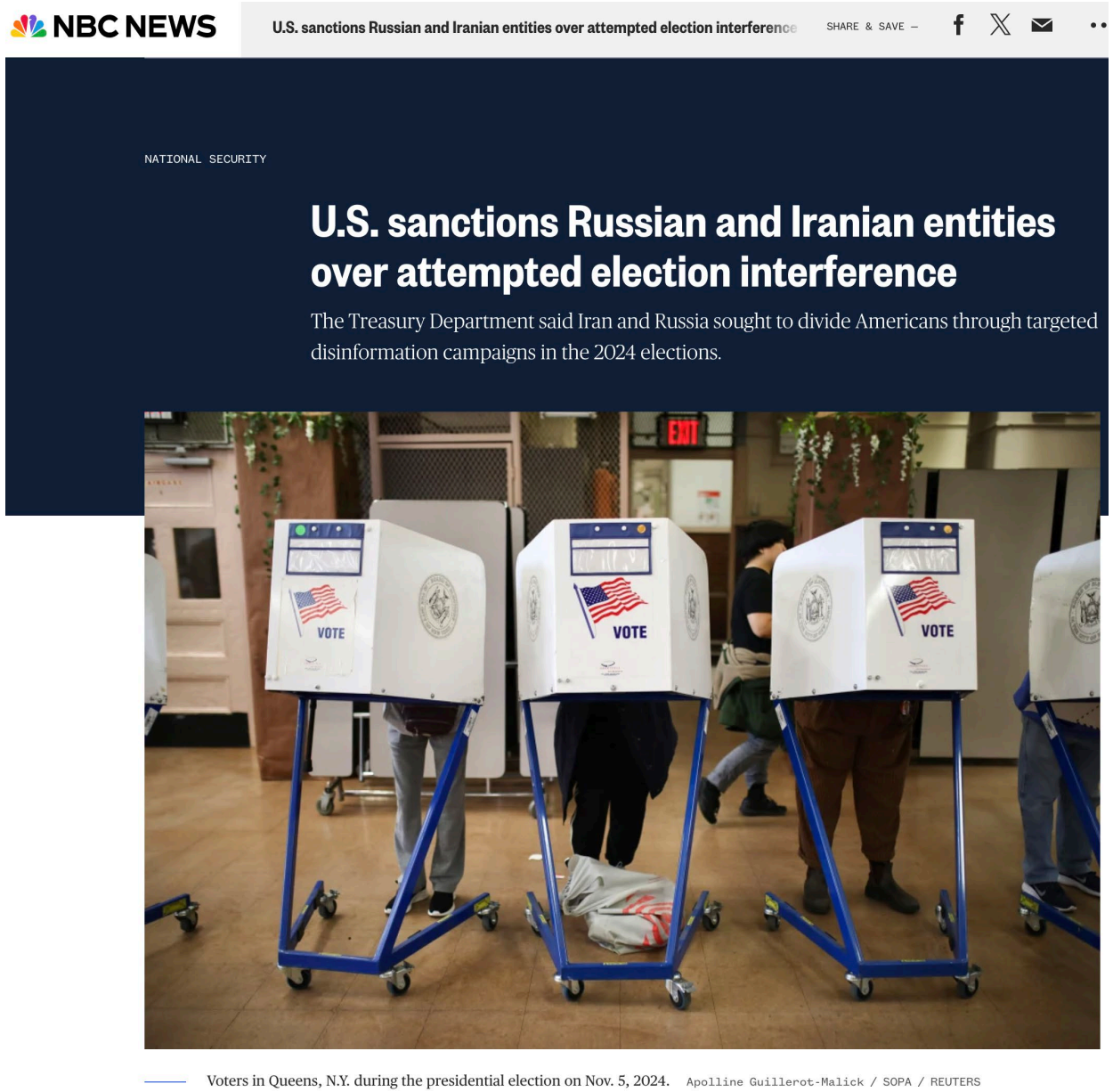
Sam Cabral
BBC News, Washington



RT boss Margarita Simonyan, seen here in 2022 with President Putin

Russia: US Presidential Election

Source: https://www.nbcnews.com/politics/national-security/us-sanctions-russian-iranian-entities-attempted-election-interference-rcna185880



NBC NEWS U.S. sanctions Russian and Iranian entities over attempted election interference SHARE & SAVE –

NATIONAL SECURITY

U.S. sanctions Russian and Iranian entities over attempted election interference

The Treasury Department said Iran and Russia sought to divide Americans through targeted disinformation campaigns in the 2024 elections.

Voters in Queens, N.Y. during the presidential election on Nov. 5, 2024. Apolline Guillerot-Malick / SOPA / REUTERS

Russia: US Presidential Election

FBI reports new hoax videos, after warnings that Russia is trying to undermine election

NOVEMBER 5, 2024 · 8:16 PM ET

Shannon Bond

Foreign adversaries are expected to boost election fraud claims after Nov. 5.

Kent Nishimura/Getty Images

https://www.npr.org/2024/11/05/g-s1-32680/2024-election-russia-iran-china-results

TALGLOBAL
Trusted Expert Solutions
Security Consulting ◆ Risk Management

RSAC 2025 Conference

Russia's Disinformation & Propaganda Ecosystem

GEC
Global Engagement Center
PILLARS OF RUSSIA'S DISINFORMATION AND PROPAGANDA ECOSYSTEM
Official Government Communications
• Kremlin or Ministry statement[1]
• Official Russian social media post[2]
• Statement or quote by Russian official[3]
State-Funded Global Messaging
• State-funded, foreign-facing media[4]
• State-funded, domestic-facing media[5]
• Foreign-based, Russian state-funded media[6]
• International Russian socio-cultural institutions[7]
Cultivation of Proxy Sources
• Russia-aligned outlets with global reach[8]
• Local language-specific outlets[9]
• Witting proliferators of Russian narratives[10]
• Unwitting proliferators of Russian narratives[11]
• Foreign state narrative amplification[12]
Weaponization of Social Media
• Infiltration of domestic conversations[13]
• Standing campaigns to undermine faith in institutions[14]
• Amplification of protests or civil discord[15]
Cyber-Enabled Disinformation
• Hack & Release[16]
• Site capture[17]
• Cloned websites[18]
• Forgeries[19]
• Disruption of official sources or objective media[20]
CONNECTION TO RUSSIA
VISIBLE
OBSCURED
DENIED

Russian Instruments Of National Power

China's Disinformation Strategies

- **National Discourse Power:** China aims to control the global narrative and establish itself as the authority on key issues. This strengthens their international influence and promotes their preferred world order.
- **Protecting Sovereignty:** Disinformation campaigns often focus on solidifying China's territorial claims, particularly regarding Taiwan, Hong Kong, Xinjiang, and Tibet. They aim to delegitimize opposing viewpoints and downplay any internal dissent.

TALGLOBAL
Trusted Expert Solutions
Security Consulting ◆ Risk Management

China’s disinformation tactics

- **Wolf Warrior Diplomacy:** Chinese diplomats aggressively defend the government's position and attack critics, often on social media. This tactic aims to silence criticism and intimidate opponents.
- **State Media Manipulation:** China uses its extensive state media apparatus to promote positive stories about the government and downplay negative news. This creates a controlled information environment within China and influences global perceptions.
- **Social Media Campaigns:** China leverages social media platforms, both domestic and foreign, to spread pro-government content and manipulate discussions. This can involve using inauthentic accounts (bots), fake news articles, and social media influencers. However, their techniques here are considered less sophisticated than those of some other actors.

China's disinformation techniques

- **Weaponizing Legality:** China uses national and international laws in unconventional ways to silence critics and control the flow of information. This can include legal threats, lawsuits, and censorship.
- **Exploiting Social Divisions:** Disinformation campaigns often target existing social cleavages within a country or region. By amplifying divisions, China weakens its opponents and creates a more favorable environment for its goals.
- **Creating a "Fake-Proof" Ecosystem:** China employs tactics like deepfakes (manipulated videos) and floods social media with disinformation to overwhelm fact-checkers and make it difficult to discern truth from falsehood.

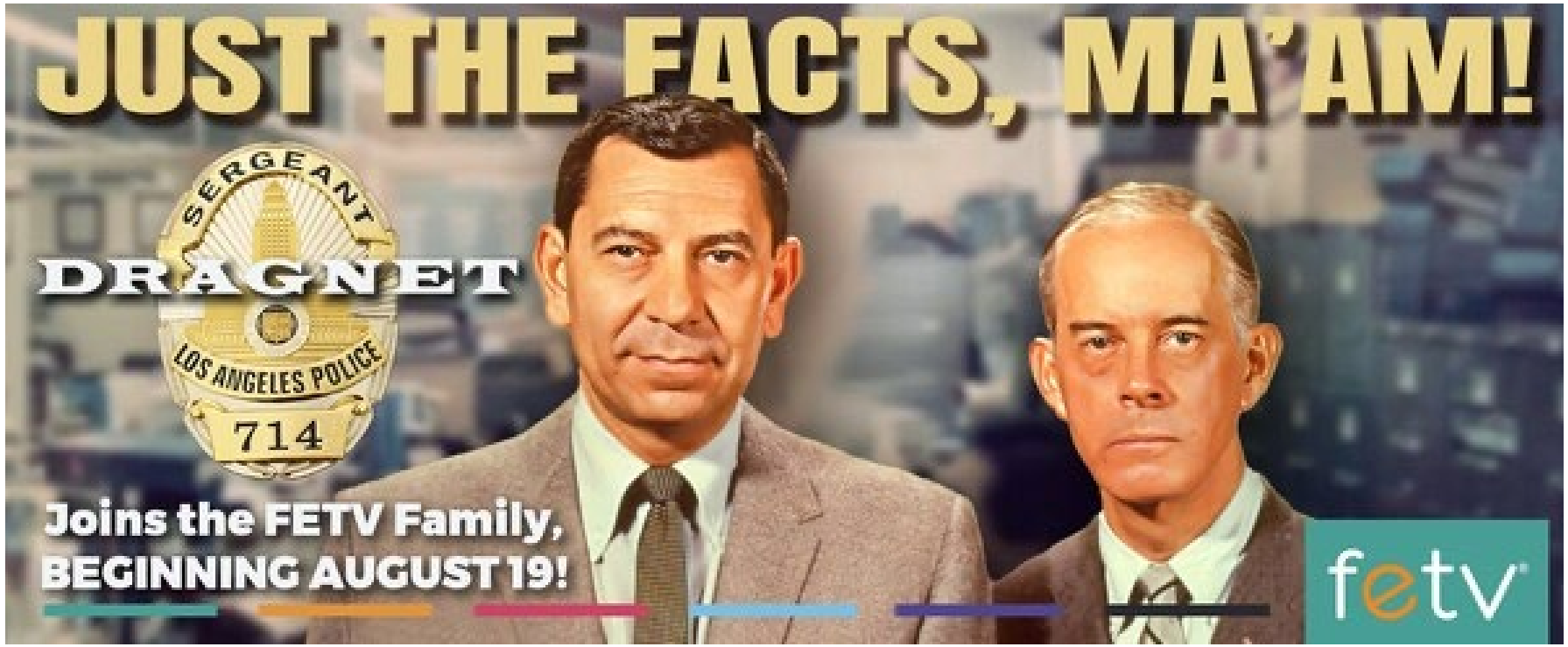
Enterprise Influence Operations (EIO)

- Defined: A coordinated strategic effort to shape perceptions and behaviors across key stakeholders to achieve business objectives.

Key Principles

- Unified Narrative
- Stakeholder Segmentation, Targeting and Responsibility
- Cross Functional Coordination
- Information Dominance
- Proactive vs. Reactive

The Story is True



Source: https://www.prnewswire.com/news-releases/dragnet-coming-to-fetv-august-19th-302201717.html

Apply Now

- Ensure that all stakeholders know what is sensitive information.
- Review the process used to determine what product and financial information is releasable to the public.
- Review or establish common ‘messages’ across the organization that further the organization’s goals.

5 Specific Actions for the Next Three Months

- Develop or review your competitive intelligence program to include profiling how your lead and potential competitors are using information to increase their revenue and/or win competitive deals from you.
- Establish periodic meetings with Analyst Firms for updates on market trends and competitive activities.
- Initiate a project to determine an objective picture of how your organization and its products are perceived by your customers and prospects.
- Provide key stakeholders with situational awareness of political developments that could impact your organization and/or your market.
- Develop an Executive Reading List

RSAC 2025 Conference

Many Voices.
One Community.

Thank You!

For More Information:

ldietz@talglobal.net